

What I claim is:

1 1. In an IEEE 802.11(b) wireless LAN, a method for accessing and analyzing the
2 contents of data packets or frames transmitted along a IEEE 802.11(b) wireless
3 communication channel, comprising the steps of:

4 establishing a direct wireless logical connection with the wireless
5 communications network;

6 receiving wirelessly, in real-time, data packets or frames transmitted in
7 the wireless communications network for all stations or devices associated
8 therewith;

9 performing over a first period of time a detailed protocol analysis on
10 the contents of the header of the data packets or frames, including analyzing
11 associated protocol layers in detail; and

12 displaying in real time the results of the analysis to a user.

1 2. The method of Claim 1, further including the steps of:

2 storing in a memory storage device, the data packets or frames
3 captured over a second period of time; and

4 performing an offline detailed analysis on the contents of the IEEE
5 802.11(b) header of the data packets or frames, and associated protocol layers,
6 stored in the memory storage device; and

7 displaying the results to the user.

1 3. The method of Claim 1, further including the step of:

2 selectively turning said detailed protocol analysis on or off for a
3 particular protocol layer, whereby for a protocol layer turned off, that layer and
4 all protocol layers above or higher than that layer are not subjected to a

5 detailed protocol analysis.

1 4. The method of Claim 1, wherein the step of performing a detailed protocol
2 analysis includes the step of generating alarms for display relating to detected
3 network and protocol errors.

1 5. The method of Claim 4, wherein the step of performing a detailed protocol
2 analysis further includes selectively turning on or off said alarm generating
3 step.

1 6. The method of Claim 4, wherein the step of performing a detailed protocol
2 analysis further includes the steps of:

3 assigning a default severity level from a plurality of available severity
4 levels for each available alarm; and

5 selectively determining whether a particular alarm type is to be logged
6 when generated.

1 7. The method of Claim 6, further including the step of selectively marking an
2 alarm as a diagnosis or a symptom dependent upon the detected severity level.

1 8. The method of Claim 1, wherein said step of displaying includes the step of
2 showing all layers of protocols analyzed for each capture of frame or data
3 packets.

1 9. The method of Claim 8, wherein said step of displaying further includes the
2 step of:

3 showing the total number of frames and octets analyzed for a selected
4 protocol layer.

10. The method of Claim 8, wherein said step of displaying includes the step of
showing for a selected protocol layer, lower layer objects linked to a current
selected object.

- 1 11. The method of Claim 8, wherein said step of displaying includes the step of
2 showing the hosts created for said IEEE 802.11(b) wireless communication
3 layer, and the attributes of said hosts, respectively.
- 1 12. The method of Claim 11, further including showing detailed statistics for each
2 selected host.
- 1 13. The method of Claim 11, further including showing attributes for each selected
2 host, including MAC address, station function, frame types, channel, network
3 types, BSSID, and SSID.
- 1 14. The method of Claim 11, further including showing the higher layer DLC
2 objects linked to selected wireless layer hosts, respectively.
- 1 15. The method of Claim 11, further including showing alarms associated with a
2 selected host.
- 1 16. The method of Claim 1, wherein said step of detailed protocol analysis
2 includes the steps of:
3 permitting a user to enter the MAC addresses of known access points
4 operating in said IEEE 802.11(b) wireless communication channel;
5 selectively activating a rogue access point detection routine;
6 checking the addresses of newly detected access points against the
7 addresses of said known access points; and
8 marking for display as a rogue access point, any access point detected
9 that is not included as a known access point.
- 1 17. A wireless network troubleshooting tool for monitoring an IEEE 802.11(b)
2 LAN wireless communication network to detect and diagnose failures in said
wireless communication network, said tool comprising:

4 a wireless network interface device operable in a promiscuous mode
5 within a wireless communications network for capturing a plurality of
6 frames or data packets transmitted through the network for all stations or
7 devices associated therewith;

8 a user interface system including input and output devices for enabling
9 a user to input and obtain information associated with said plurality of
10 captured frames;

11 a memory storage device for storing said plurality of captured frames
12 as received from said wireless network interface device; and

13 a programmable processor unit connected to said wireless network
14 interface device, said user interface system, and said memory storage device,
15 said processor being programmed to execute a routine comprising the steps of:

16 establishing a direct wireless logical connection with said
17 wireless communications network via the network interface device;

8 receiving wirelessly, in real-time, frames transmitted in the
9 wireless communications network via direct wireless logical connection;

0 receiving from said user, via said user interface ,configuration
1 parameters;

2 performing, through use of said configuration parameters a
3 detailed protocol analysis on the contents of respective headers of the
4 captured data packets or frames, including associated protocol layers,
5 respectively; and

displaying the results of the analysis to the user in real-time.